UNITED STATES PATENT AND TRADEMARK OFFICE

mn

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/810,308	03/26/2004	Michael John Wray	B-5404 621794-8	7996

7590   06/12/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER
YOUNG, NICOLE M

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
06/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/810,308	WRAY, MICHAEL JOHN
	Examiner	Art Unit
	Nicole M. Young	2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>*26 March 2004*</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>*1-13,15 and 16*</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>*1-13, 15-16*</u> is/are rejected.

7)☐ Claim(s) <u>*3, 6, and 8*</u> is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>*26 March 2004*</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

       1.☒ Certified copies of the priority documents have been received.

       2.☐ Certified copies of the priority documents have been received in Application No. _____.

       3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date <u>*11/18/2004*</u>.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

Specification

The disclosure is objected to because of the following informalities: '

Page 1 "The or each compartment"

Page 3 "preferably the or each security"

Page 11 "Monitoring mean s may"

The disclosure is objected to because it contains an embedded hyperlink and/or

other form of browser-executable code. Applicant is required to delete the embedded

hyperlink and/or other form of browser-executable code. See MPEP § 608.01, for

example, page 1 www.trustedpc.org.

Appropriate correction is required.

Claim Objections

Claims 3, 6, 8, objected to because of the following informalities:

Claim 3 "the or each security rule"

Claim 6 "operate" should be "operates"

Claim 8 "chrooted" is not a word.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly
claiming the subject matter which the applicant regards as his invention.

Claim 8 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite

for failing to particularly point out and distinctly claim the subject matter which applicant

regards as the invention. As stated in the objection to claim 8, the Applicant uses the

term "chrooted" which is not a proper word.

Claims 11-13 recite the limitation ""said execution control rule". There is

insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-7, 9-13, and 15-16 are rejected under 35 U.S.C. 102(e) as being

anticipated by **Wiseman et al. (US 7,216,3696)**.

Claim 1 discloses (original) a system comprising a trusted computing platform and one

or more logically protected computing environments, each of which is associated with at

least one service or process supported by said system (Fig. 1 and associated text show

a system with a TPM and at least one service or process), the system being arranged to

load onto said trusted computing platform data defining a predetermined security policy

defining security to be applied to one or more of the at least one service or process

when said service or process is started (Figs 3A and 3B show the loading of security

policies when the OS is started. Particularly, blocks 321 and 323 show loading the

policies into the TPM as in column 7 lines 25-38. These policies are then applied and if

they are not satisfied an alert is set off as in column 7 lines 39-48).

Claim 2 discloses (original) a system according to claim 1 wherein the policy included

one or more security rules for controlling operation of logically protected computing

environments (Column 3 lines 52-63 wherein the Examiner interprets "information

placed by the platform owner" to be "security rules").

Claim 3 discloses (original) a system according to claim 2 wherein the or each security

rule for at least one of the logically protected environments will include an execution

control rule which defines the security attributes (Column 3 lines 52-63 especially "The

policy table 118 contains policies which the platform 102 must adhere during the

initialization/boot process", and the policy table is validated by the DIR 120 which

resides in the TPM).

Claim 4 discloses (original) a system according to claim 3, wherein said security

attributes include or comprise one or more capabilities to be provided to the respective

logically protected computing environment when said service or process is started

(Column 3 lines 52-63 especially "The policy table 118 contains policies which the

platform 102 must adhere during the initialization/boot process", and the policy table is

validated by the DIR 120 which resides in the TPM).

Claim 5 discloses (original) a system according to claim 3, wherein said security

attributes include or comprise one or more functions which change or modify the

capabilities of the respective logically protected computing environment when said

service or process is started (Column 3 lines 52-63 especially "The policy table 118

contains policies which the platform 102 must adhere during the initialization/boot

process", and the policy table is validated by the DIR 120 which resides in the TPM.

The computing environment will be modified by the alerting and stopping of the booting

process as in Figs 3A and 3B and also by disabling the TPM as in column 7 lines 25-

38).

Claim 6 discloses (original) a system according to claim 3, wherein when a service or

process is started said security attribute operate to cause the service or process to be

placed and run in a specified logically protected computing environment (Column 3 lines

52-63 especially "The policy table 118 contains policies which the platform 102 must

adhere during the initialization/boot process", and the policy table is validated by the

DIR 120 which resides in the TPM).

Claim 7 discloses (original) a system according to claim 3, wherein said security

attributes operate to modify a user id, a group id or a logically protected computing

environment in which a service or process is to be run (Column 3 lines 52-63 especially

"The policy table 118 contains policies which the platform 102 must adhere during the

initialization/boot process", and the policy table is validated by the DIR 120 which

resides in the TPM. The computing environment will be modified by the alerting and

stopping of the booting process as in Figs 3A and 3B and also by disabling the TPM as

in column 7 lines 25-38).

Claim 9 discloses (original) a system according to claim 5, wherein said execution

control rule can raise or lower a specified capability (Column 3 lines 52-63 especially

"The policy table 118 contains policies which the platform 102 must adhere during the

initialization/boot process", and the policy table is validated by the DIR 120 which

resides in the TPM. The computing environment will be modified by the alerting and

stopping of the booting process as in Figs 3A and 3B and also by disabling the TPM as

in column 7 lines 25-38.).

Claim 10 discloses (currently amended) a system according to ~~claim 5 or claim 9~~ claim

5, wherein the security attributes operate to filter a set of capabilities of a logically

protected computing environment and modifying only one or more of said capabilities as

selected by said filtering means (Column 3 lines 52-63 especially "The policy table 118

contains policies which the platform 102 must adhere during the initialization/boot

process", and the policy table is validated by the DIR 120 which resides in the TPM.

The computing environment will be modified by the alerting and stopping of the booting

process as in Figs 3A and 3B. The Examiner determines the process of comparing and

alerting the system if a policy is violated to be filtering.).

Claim 11 discloses (currently amended) a system according to ~~any one of the~~

~~proceeding claims~~ claim 1, wherein said execution control rule specifies the service or

process to which it applies by identifying the associated logically protected computing

environment, with the effect that said rule applies only to services or processes

specifying that logically protected computing environment (Column 3 lines 52.).

Claim 12 discloses (currently amended) a system according to ~~any one of the proceeding~~

~~claims~~ claim 1 the files making up a service or process to which said execution control

rule applies are of read only configuration.

Claim 13 discloses (currently amended) a system according to ~~any one of the~~ ~~proceeding claims~~ claim 1, including means for monitoring operations performed by the system which modify names of files making up services or programs to which said execution control rule applies (Column 3 lines 20-22).

14. (canceled)

Claim 15 discloses (original) a method of applying a security policy in a system including a trusted computing platform and one or more logically protected computing environments, each of which is associated with at least one service or process supported by said system, the method including the steps of starting a service or process associated with at least one of the logically protected computing environments; and controlling the operation of the at least one logically protected environment by applying, upon starting of the service or process, security attributes to the service or process(Fig. 1 and associated text show a system with a TPM and at least one service or process. Figs 3A and 3B show the loading of security policies when the OS is started. Particularly, blocks 321 and 323 show loading the policies into the TPM as in column 7 lines 25-38. These policies are then applied and if they are not satisfied an alert is set off as in column 7 lines 39-48).

Claim 16 (original) discloses a method according to claim 15 wherein the attributes are defined by execution control rules, which are included in security rules implementing at least part of the policy (Column 3 lines 52-63 especially "The policy table 118 contains policies which the platform 102 must adhere during the initialization/boot process", and the policy table is validated by the DIR 120 which resides in the TPM).

17. (canceled)

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Wiseman et al. (US 7,216,3696) hereinafter Wiseman as applied to **claims 1-7, 9-13,**

and 15-16 above, and further in view of **Challener et al. (US 2003/0188179)** hereinafter

Challener.

Claim 8 (original) discloses a system according to claim 3, wherein said security

attributes operate to define a directory to which the service or process is to be chrooted

(The Examiner interprets this claim to refer to the Linux command "chroot". Wiseman

teaches Operating Systems (column 1 lines 36-40) but does not teach Linux

specifically. Challener teaches the Linux operating system in paragraph [0006]. The

motivation to combine would be Challener paragraph [0006], "the creation of the trusted

computer platform, which is typically operated with Linux operating system." The

trusted computer platform of Challener is interpreted to be equivalent to the trusted

computer platform of Wiseman).

Note: Examiner has pointed out particular references contained in the prior arts of

record and in the body of this action for the convenience of the applicant. Although the

specified citations are representative of the teachings in the art and are applied to the

specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable to the limitations of the claims. It is respectfully requested from the applicant, in preparing for response, to consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the Examiner.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nicole M. Young whose telephone number is 571-270-1382. The examiner can normally be reached on Monday through Friday, alt Fri off, 8:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NMY
06/04/2007

TAGHI ARANI
PRIMARY EXAMINER